REMARKS

The Applicants and the undersigned thank Examiner Son for his time and consideration given during the telephonic interview of August 15, 2006, and for his careful review of this application. After entry of this Amendment, Claims 1-59 are pending in the present application, with Claims 1, 16, 27, 34, and 49 being independent. Applicants have amended Claims 1, 16, 27, 34, and 49 herein. The Applicants believe that no new matter has been added to this application.

Consideration of the present application is respectfully requested in light of the above amendments to the application and in view of the following remarks

Summary of Telephonic Interview of August 15, 2006

The Applicants and the undersigned thank Examiner Son for his time and consideration given during the telephonic interview of August 15, 2006. During this telephonic interview, the differences between the prior art of record, U.S. Patent No. 6,088,804 issued to Hill (hereinafter the "Hill reference"), and proposed amendments to the claims were discussed.

The Applicants' representative explained that the Hill reference does not provide any teaching of analyzing and filtering security event data, as recited in amended independent Claims 1, 16, 27, 34, and 49.

Examiner Son understood the differences explained by Applicants' representative with respect to the Hill reference and he understood what inventive features the Applicants are trying to claim. Examiner Son indicated that the Applicants should further define the term "security event data" to clarify the type of data that is being analyzed and filtered. Examiner Son indicated that he would conduct an updated search on the technology when the Applicants submit a formal amendment containing amended language as discussed during the telephonic interview.

The Applicants and the undersigned request Examiner Son to review this interview summary and to approve it by writing "Interview Record OK" along with his initials and the date next to this summary in the margin as discussed in MPEP § 713.04.

Claim Rejections

In the Office Action dated April 20, 2006, the Examiner rejected Claims 1-11, 13-22, 24-44, 46-55, and 57-59 under 35 U.S.C. §102(e) as being anticipated by the Hill reference. Furthermore, the Examiner rejected Claims 12, 23, 45, and 56 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Hill in view of an alleged obviousness rejection at the time of the invention for one having ordinary skill in the art.

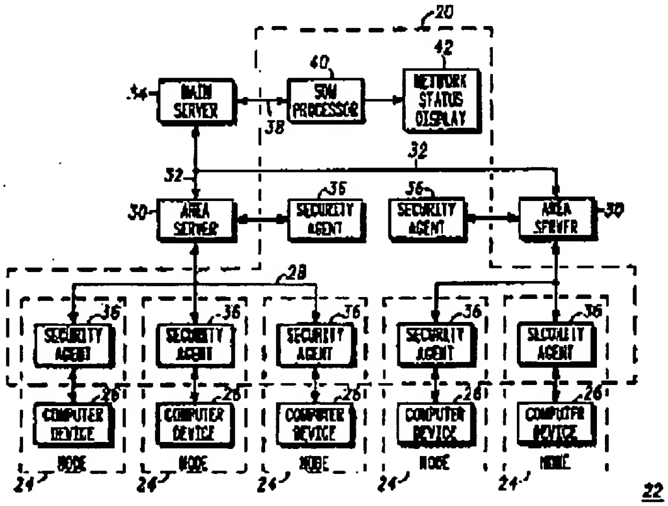
The Applicants respectfully offers remarks to traverse these rejections. The Applicants will address each independent claim separately as the Applicants believes that each independent claim is separately patentable over the prior art of record.

Independent Claim 1

The rejection of Claim 1 is respectfully traversed. It is respectfully submitted that the Hill reference fails to describe, teach, or suggest the combination of: (1) generating security event data comprising a plurality of alerts with a plurality of security devices at a first location in response to detecting a security event in a distributed computing environment; (2) providing one or more variables operable for analyzing and filtering the security event data, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event; (3) creating scope criteria by selecting one or more of the variables operable for analyzing and filtering the security event data; (4) collecting the security event data generated by the plurality of security devices located at the first location; (5) storing the collected security event data at a second location; (6) analyzing and filtering the collected security event data with the scope criteria to produce result data; (7) transmitting the result data to one or more clients; and (8) displaying the result data comprising filtered alerts based on the scope criteria, as recited in amended independent Claim 1.

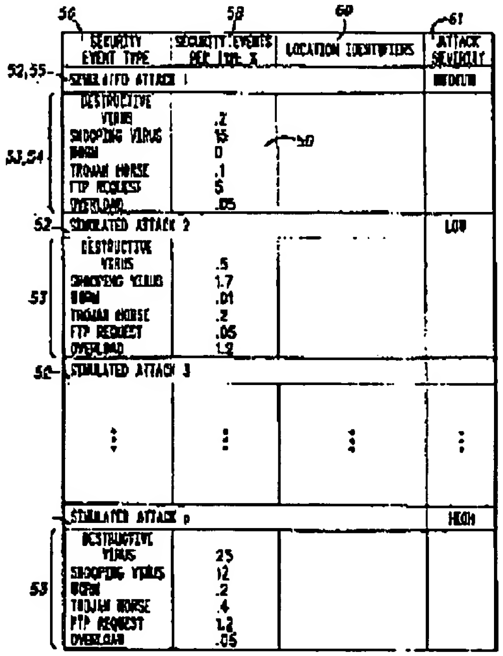
The Hill Reference

The Hill reference describes a dynamic network security system (20) that responds to a security attack on a computer network (22) having a multiplicity of computer nodes (24). The security system (20) includes a plurality of security agents (36) that concurrently detect occurrences of security events on associated computer nodes (24). A processor (40) processes the security events that are received from the security agents (36) to form an attack signature of the attack. A network status display (42) displays multi-dimensional attack status information representing the attack in a two dimensional image to indicate the overall nature and severity of the attack. See Figure 1 of the Hill system reproduced below.



As shown in Figure 3 of the Hill reference below, a database (48) maintains the simulated attack information for a plurality of simulated attacks (52). Each of the simulated attacks (52) is a prediction of an attack type that may occur on network (22). Simulated attacks (52) are generated by an operator and stored in database (48). Each simulated attack (52) contains a training signature (53) that is defined by a plurality of security events (50) of at least one security event type (56). Security events (50) are presented in database (48) in a column (58) as a percentage of security events per event type.

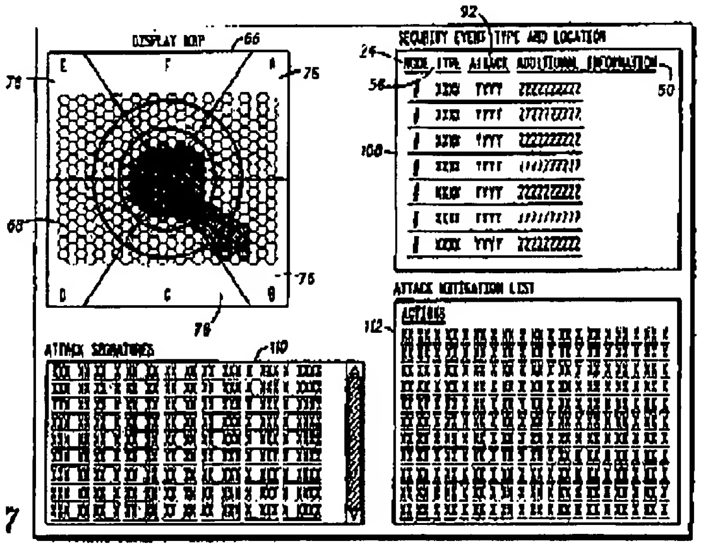
In addition to security event types (56) and percentage of security events (50) per event type in column (58), training signatures (53) include location identifiers (60). Location identifiers (60) identify the nodes (24) in network (22) where security events may take place. Location identifiers (60) are important for ascertaining an attack severity (61) for each of simulated attacks (52). Attack severity (61) is a level of security breach that one of simulated attacks (52) could cause computer network (22).



SECURITY EVENT TYPE	SECURITY EVENTS PER TYPE %	LOCATION IDENTIFIERS	ATTACK SEVERITY
SIMULATED ATTACK 1			MEDIUM
DESTRUCTIVE VIRUS	.2		
SNOOPING VIRUS	15		
WORM	0		
TROJAN HORSE	.1		
FTP REQUEST	5		
OVERLOAD	.05		
SIMULATED ATTACK 2			LOW
DESTRUCTIVE VIRUS	.5		
SNOOPING VIRUS	1.7		
WORM	.01		
TROJAN HORSE	.2		
FTP REQUEST	.05		
OVERLOAD	1.2		
SIMULATED ATTACK 3			
⋮	⋮	⋮	⋮
SIMULATED ATTACK p			HIGH
DESTRUCTIVE VIRUS	25		
SNOOPING VIRUS	12		
WORM	.2		
TROJAN HORSE	.4		
FTP REQUEST	1.2		
OVERLOAD	.05		

FIG. 3

As shown in Figure 7 of the Hill reference below, a network status display (42) displays multi-dimensional attack status information in a two dimensional image to indicate the overall nature and severity of an attack. The network status display (42) presents a display map (66) and an attack status information list (108) showing security event type (56) and location identifiers (60) for an example attack (92). The network status display (42) also presents an attack signature log (110) which provides current and historical perspective on a given attack record at various sample times. The attack signatures in log (110) are the text equivalent of the two dimensional image as highlighted in display map (66). In addition, the network status display (42) includes an attack mitigation list (112) which is a catalogue of actions that a network manager may take in order to mitigate the example attack (92).



42

FIG. 7

In summary, the Hill reference teaches generating simulated attacks that may occur on the network. The simulated attacks comprise training signatures that define what type of security events are present in each attack. In response to the simulated attacks, the system in the Hill reference can subsequently be trained to detect and respond to actual security attacks by monitoring and analyzing the network traffic data. In response to an actual security attack, the system in the Hill reference can respond with an action that corresponds to a simulated attack that is stored in the database. Thereafter, the Hill reference can present a display map containing attack information. Thus, the Hill reference fails to teach for providing one or more variables operable for analyzing and filtering the security event data and it fails to teach creating scope criteria by selecting one or more of the variables operable for analyzing and filtering the security event data and analyzing and filtering the collected security event data with the scope criteria to produce result data, wherein the security event data comprises a plurality of alerts with a plurality of security devices at a first location in response to detecting a security event in a distributed computing environment

Therefore, the Hill reference fails to teach generating security event data comprising a plurality of alerts with a plurality of security devices at a first location in response to detecting a security event in a distributed computing environment, and providing one or more variables operable for analyzing and filtering the security event data, as recited in amended independent Claim 1. Furthermore, the Hill reference fails to teach creating scope criteria by selecting one or more of the variables operable for analyzing and filtering the security event data and analyzing and filtering the collected security event data with the scope criteria to produce result data, as recited in amended independent Claim 1.

In light of the differences between amended independent Claim 1 and the Hill reference, one of ordinary skill in the art recognizes that the Hill reference fails to describe, teach, or suggest the recitations as set forth in amended independent Claim 1. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 16

The rejection of Claim 16 is respectfully traversed. It is respectfully submitted that the Hill reference fails to describe, teach, or suggest the combination of: (1) generating security event data comprising a plurality of alerts with the plurality of security devices at a first location in response to detecting a security event in a distributed computing environment; (2) providing one or more variables operable for analyzing and filtering the security event data, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event; (3) creating scope criteria by selecting one or more of the variables operable for analyzing and filtering the security event data; (4) collecting security event data at a second location; (5) applying the scope criteria to the security event data at a third location to produce result data; (6) transmitting the result data to one or more clients; and (7) displaying the result data comprising filtered alerts based on the scope criteria, as recited in amended independent Claim 16.

Similar to the analysis of independent Claim 1, the Hill reference fails to teach generating security event data comprising a plurality of alerts with a plurality of security devices at a first location in response to detecting a security event in a distributed computing environment, and then providing one or more variables operable for analyzing and filtering the security event data, as recited in amended independent Claim 16. Furthermore, the Hill reference fails to teach creating scope criteria by selecting one or more of the variables operable for analyzing and filtering the security event data, as recited in amended independent Claim 16.

In light of the differences between amended independent Claim 16 and the Hill reference, one of ordinary skill in the art recognizes that the Hill reference fails to describe, teach, or suggest the recitations as set forth in amended independent Claim 16. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 27

The rejection of Claim 27 is respectfully traversed. It is respectfully submitted that the Hill reference fails to describe, teach, or suggest a system that includes: (1) a plurality of security devices operable for generating security event data comprising a plurality of alerts that are generated in response to detecting a security event in a distributed computing environment; (2) an event manager coupled to the security devices, the event manager operable for collecting the security event data from the security devices and analyzing and filtering the security event data with scope criteria comprising one or more definable variables operable for analyzing and filtering the security event data, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event; and (3) one or more clients coupled to the event manager operable to perform an action in response to receiving analyzed security event data from the event manager, as recited in amended independent Claim 27.

Similar to the analysis of independent Claim 1, the Hill reference fails to teach generating security event data comprising a plurality of alerts that are generated in response to detecting a security event in a distributed computing environment and analyzing and filtering the security event data with scope criteria comprising one or more definable variables operable for analyzing and filtering the security event data, as recited in amended independent Claim 27.

In light of the differences between amended independent Claim 27 and the Hill reference, one of ordinary skill in the art recognizes that the Hill reference fails to describe, teach, or suggest the recitations as set forth in amended independent Claim 27. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 34

The rejection of Claim 34 is respectfully traversed. It is respectfully submitted that the Hill reference fails to describe, teach, or suggest the combination of: (1) generating security event data comprising a plurality of alerts with a plurality of security devices at a first location in response to detecting a security event in a distributed computing environment; (2) providing one or more variables operable for analyzing and filtering the security event data, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event; (3) creating scope criteria by selecting one or more of the variables operable for analyzing and filtering the security event data; (4) collecting the security event data at a second location; (5) analyzing and filtering the collected security event data with the scope criteria at a third location to produce result data; (6) transmitting the result data to one or more clients; and (7) rendering the result data, in a manageable format for the one or more clients, as recited in amended independent Claim 34.

Similar to the analysis of independent Claim 1, the Hill reference fails to teach generating security event data comprising a plurality of alerts with a plurality of security devices at a first location in response to detecting a security event in a distributed computing environment and then providing one or more variables operable for analyzing and filtering the security event data, as recited in amended independent Claim 34. Furthermore, the Hill references fails to teach creating scope criteria by selecting one or more of the variables operable for analyzing and filtering the security event data and analyzing and filtering the collected security event data with the scope criteria at a third location to produce result data, as recited in amended independent Claim 34.

In light of the differences between amended independent Claim 34 and the Hill reference, one of ordinary skill in the art recognizes that the Hill reference fails to describe, teach, or suggest the recitations as set forth in amended independent Claim 34. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 49

The rejection of Claim 49 is respectfully traversed. It is respectfully submitted that the Hill reference fails to describe, teach, or suggest the combination of: (1) generating security event data with a plurality of security devices in response to detecting a security event in a distributed computing environment, the security event data comprising a plurality of alerts; (2) transferring the security event data for storage in a database; (3) applying a scope criteria comprising one or more definable variables to the security event data for analyzing and filtering the security event data to produce a result, the variables comprising at least one of a location of a security event, a source of security event, a destination address of the security event, a security event type, a priority of a security event, and an identification of a system that detected a security event; (4) accessing the result with one or more clients coupled to an application server; and (5) displaying the result data comprising filtered alerts based on the scope criteria, as recited in amended independent Claim 49.

Similar to the analysis of independent Claim 1, the Hill reference fails to teach generating security event data with a plurality of security devices in response to detecting a security event in a distributed computing environment, the security event data comprising a plurality of alerts and applying a scope criteria comprising one or more definable variables to the security event data for analyzing and filtering the security event data to produce a result, as recited in amended independent Claim 49.

In light of the differences between amended independent Claim 49 and the Hill reference, one of ordinary skill in the art recognizes that the Hill reference fails to describe, teach, or suggest the recitations as set forth in amended independent Claim 49. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Dependent Claims 2-15, 17-26, 28-33, 35-48, and 50-59

The Applicants respectfully submit that the above-identified dependent claims are allowable because the independent claims from which they depend are patentable over the cited prior art reference. The Applicants also respectfully submit that the recitations of these dependent claims are of patentable significance.

In view of the foregoing, the Applicants respectfully request that the Examiner withdraw the pending rejections of dependent Claims 2-15, 17-26, 28-33, 35-48, and 50-59.

CONCLUSION

Applicants submit the foregoing as a full and complete response to the Non-Final Office Action dated April 20, 2006. The Applicants and the undersigned thank Examiner Son for consideration of these remarks. Applicants submit that this Amendment places the application in condition for allowance and respectfully request such action.

If any issues exist that can be resolved with an Examiner's Amendment or a telephone conference, please contact the undersigned at 404.572.4647.

Respectfully submitted,

Kerry L. Broome

Kerry L. Broome
Reg. No. 54,004

KING & SPALDING LLP
1180 Peachtree Street, 34th Floor
Atlanta, Georgia 30309
(404) 572-4600
K&S Docket: 05456.105005